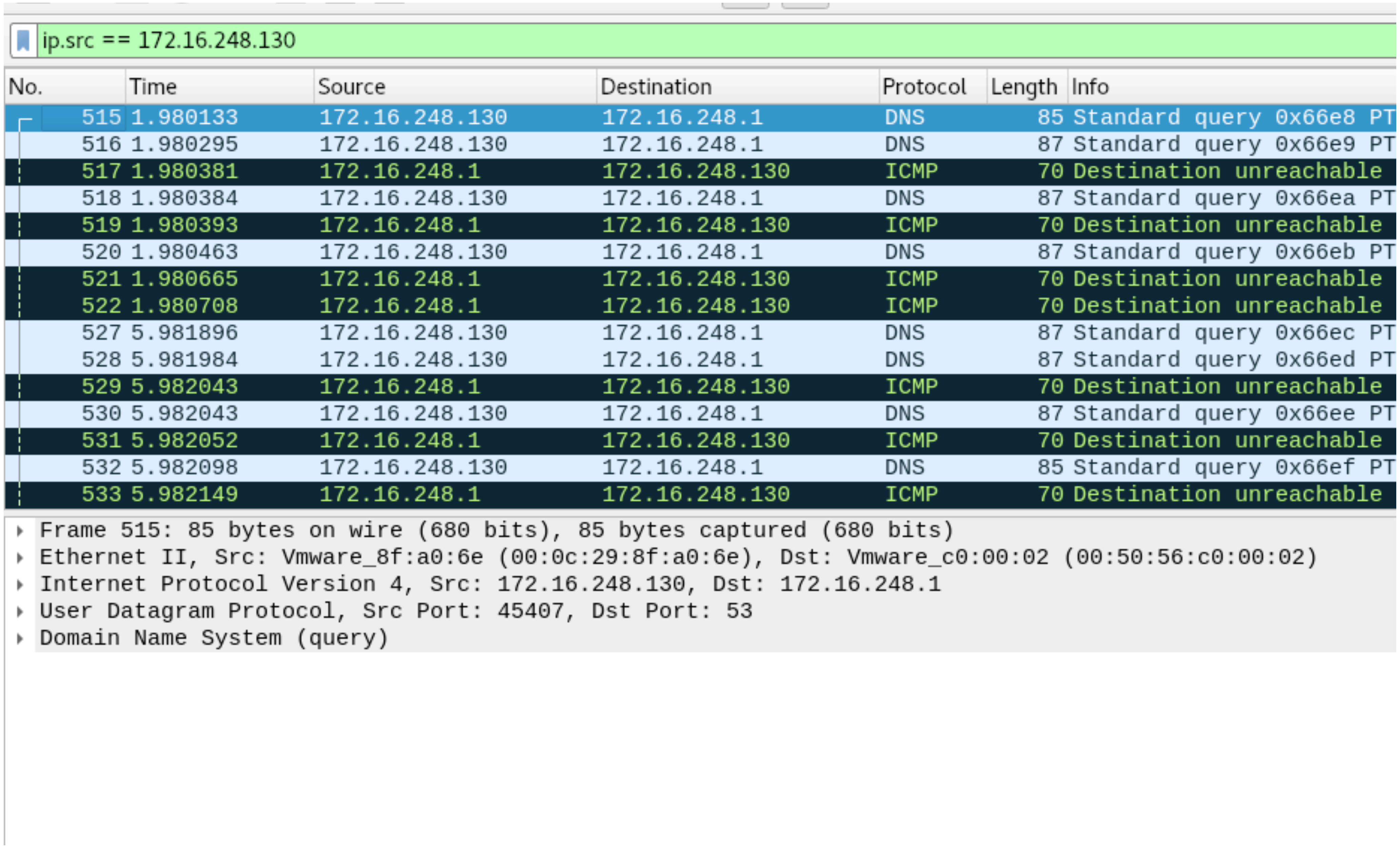
Technial Cybersecurity

ARP Session Hijacking

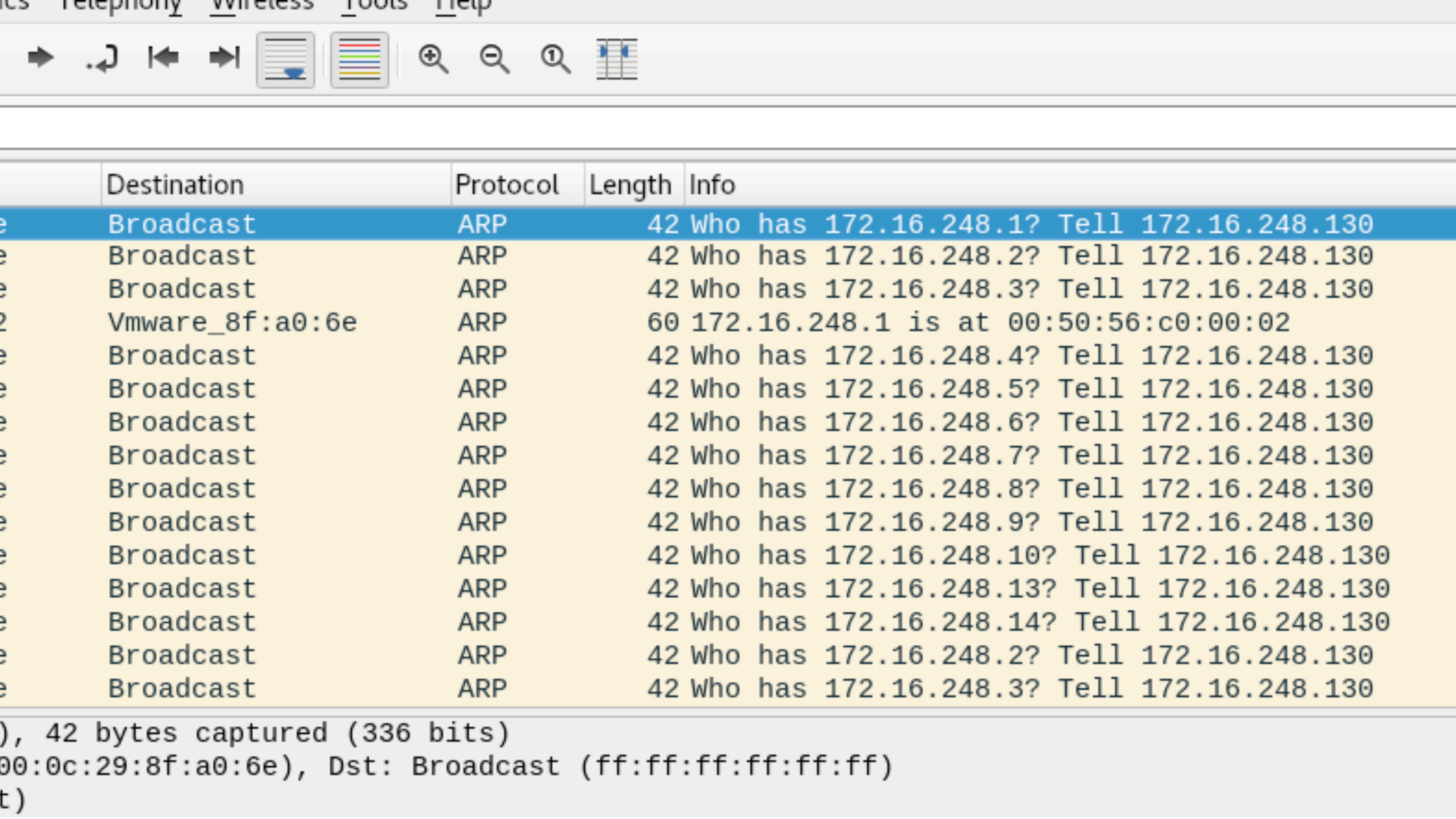


```
ip.src == 172.16.248.130

No.   Time      Source          Destination     Protocol  Length Info
  515 1.980133  172.16.248.130  172.16.248.1    DNS       85 Standard query 0x66e8 PT
  516 1.980295  172.16.248.130  172.16.248.1    DNS       87 Standard query 0x66e9 PT
  517 1.980381  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable
  518 1.980384  172.16.248.130  172.16.248.1    DNS       87 Standard query 0x66ea PT
  519 1.980393  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable
  520 1.980463  172.16.248.130  172.16.248.1    DNS       87 Standard query 0x66eb PT
  521 1.980665  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable
  522 1.980708  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable
  527 5.981896  172.16.248.130  172.16.248.1    DNS       87 Standard query 0x66ec PT
  528 5.981984  172.16.248.130  172.16.248.1    DNS       87 Standard query 0x66ed PT
  529 5.982043  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable
  530 5.982043  172.16.248.130  172.16.248.1    DNS       87 Standard query 0x66ee PT
  531 5.982052  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable
  532 5.982098  172.16.248.130  172.16.248.1    DNS       85 Standard query 0x66ef PT
  533 5.982149  172.16.248.1    172.16.248.130  ICMP      70 Destination unreachable

▸ Frame 515: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
▸ Ethernet II, Src: Vmware_8f:a0:6e (00:0c:29:8f:a0:6e), Dst: Vmware_c0:00:02 (00:50:56:c0:00:02)
▸ Internet Protocol Version 4, Src: 172.16.248.130, Dst: 172.16.248.1
▸ User Datagram Protocol, Src Port: 45407, Dst Port: 53
▸ Domain Name System (query)
```

What is ARP?

ARP == Address Resolution Protocol

Remember our PCAP from the third module? Looked like this?



	Destination	Protocol	Length	Info
e	Broadcast	ARP	42	Who has 172.16.248.1? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.2? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.3? Tell 172.16.248.130
2	Vmware_8f:a0:6e	ARP	60	172.16.248.1 is at 00:50:56:c0:00:02
e	Broadcast	ARP	42	Who has 172.16.248.4? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.5? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.6? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.7? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.8? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.9? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.10? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.13? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.14? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.2? Tell 172.16.248.130
e	Broadcast	ARP	42	Who has 172.16.248.3? Tell 172.16.248.130

```
), 42 bytes captured (336 bits)
00:0c:29:8f:a0:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
t)
```

ARP identifies IP addresses

USED TO RESOLVE IP TO MAC ADDRESSES

- Only see ARP traffic on subnets

THE WAY IT **SHOULD** WORK

- Computer A (IP: A.B.C.D) has a packet for computer B (IP: A.B.C.E)

1. *Computer A*: Hey everybody, who’s A.B.C.E? (**ARP Request**)
2. *Computer B*: Yo! I’m A.B.C.E, and you can use my MAC address of XX:XX:XX:XX:XX:XX, send me your stuff! (**ARP Reply**)
3. *Computer A*: Cool; Hey gateway please send this stuff to XX:XX:XX:XX:XX:XX! (**Not ARP; TCP or UDP or something else**)
4. *Gateway*: Sure thing, and I’ll remember that A.B.C.E is XX:XX:XX:XX:XX:XX in case anybody asks again. (**Caching**)

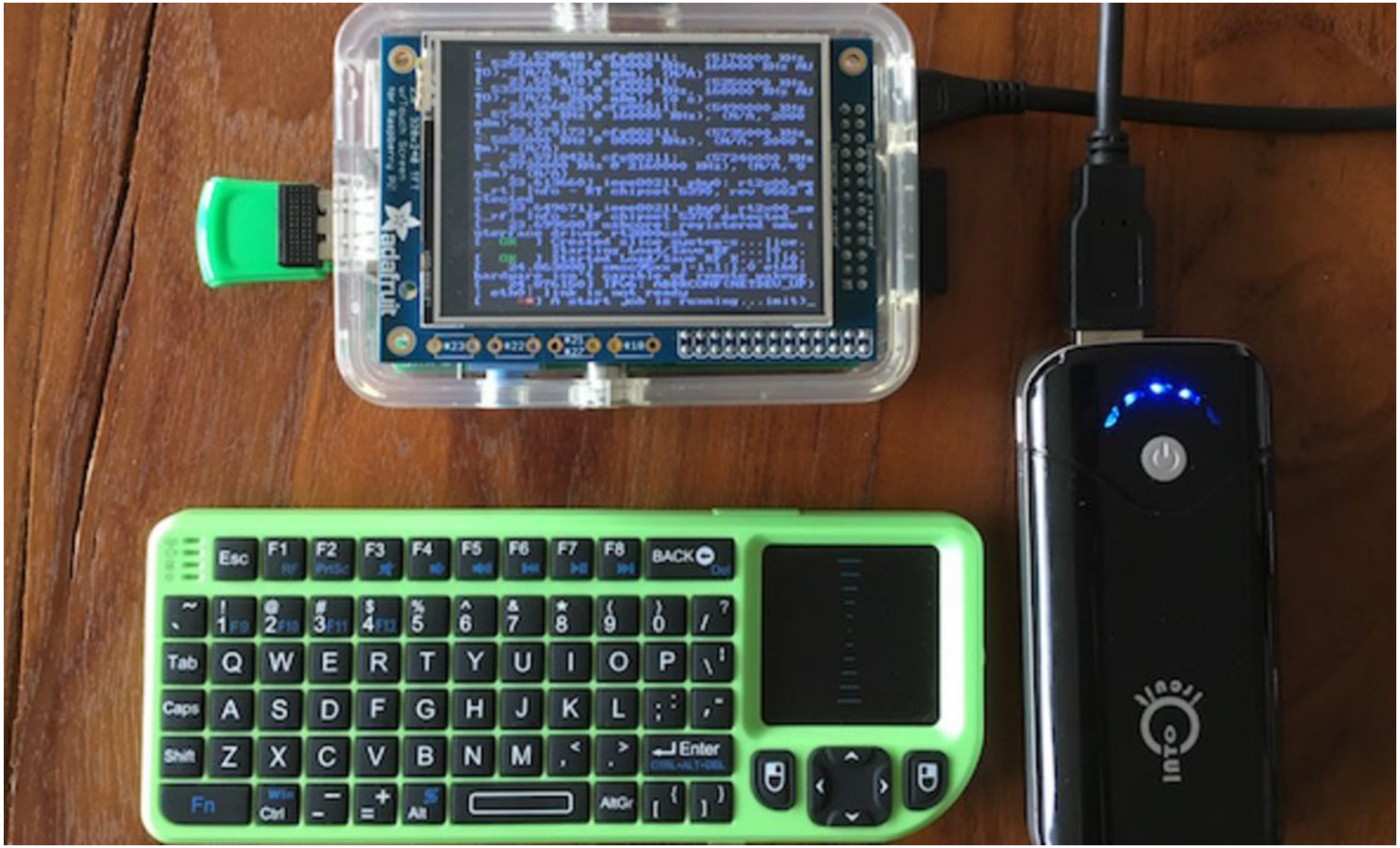
What about this?

SOMETIME LATER…

1. *Attacker*: HEY EVERYBODY I'M A.B.C.E AND MY MAC ADDRESS IS YY:YY:YY:YY:YY:YY!!!!! (**ARP Replies**)
2. *Gateway*: Okay, okay, you're A.B.C.E, sure. Geez. (**Caching**)
3. *Attacker*: EVERYBODY I'M THE GATEWAY TOO!! (**ARP Replies**)
4. *Everybody*: Got it, you're a jerk, but you're also my gateway. (**Caching**)

Now, the gateway sends everything to the attacker, who forwards to others. And others send to the attacker, who forwards to the *real* gateway.

The attacker now has a *man-in-the-middle* (MitM) position and can intercept all communications.



Raspberry Pi

How about a small portable hacking station?

Pwn Plug

And another!

Pi-Hole

And another!

Hiding network access devices isn’t that hard.

Protection

NEED TO KNOW WHAT IS ON YOUR NETWORK!

- Remember NMAP? Defenders need to use it too.
- Active probing and passive monitoring
- Automated auditing and record examination

Next, let’s talk passwords.